IN THE CLAIMS

This listing of the claims will replace all prior versions, and listings, of the claims in this application.

1. (Currently Amended) A method, comprising:
    for packets comprising binding update messages:

    generating validity information for a-the packets, wherein the validity information for
    a packet comprises all necessary information required to perform a validity
    check of the packet, the validity information comprising algorithm information
    to be used to perform the validity check of the packet and algorithm
    initialization information, the validity information further comprising public
    key information of a sending node comprising an address in a database of a
    server from which the public key of the sending node can be obtained, where
    no pre-established security association is needed to verify the packet; and

    generating a-packet headers, comprising the validity information; and

    for packets not comprising the binding update messages, generating a packet header
    without the validity information; and

    sending the-packets including the corresponding packet header-headers from a first
    network node-to a second-receiving network node.

2. (Previously Presented) The method according to claim 1, wherein the generating of the validity information comprises generating security information indicating security services applied to the packet.

3.   (Cancelled)

4.   (Previously Presented) The method according to claim 1, wherein the generating of the algorithm information comprises generating the algorithm information which indicates an algorithm to be used to perform the validity check of the packet.

5.-10. (Cancelled).

11.   (Previously Presented) The method according to claim 1, wherein the generating of the public key information comprises generating public key verification information indicating information in order to verify that the public key actually belongs to the sending node.

12.   (Previously Presented) The method according to claim 1, wherein the generating of the validity information comprises generating an information item to prevent replay attacks.

13.   (Previously Presented) The method according to claim 12, wherein the generating of the information item comprises including in the information item an indication of a procedure to be used for anti replay attacks.

14.   (Previously Presented) The method according to claim 12, wherein the generating of the information item comprises including in the information item a time stamp.

15.   (Previously Presented) The method according to claim 1, further comprising:

        signing the packet using a private key corresponding to the public key indicated by the

        validity information.   .

16-17. (Cancelled)

18.   (Currently Amended) An apparatus, comprising:

        validity information generating means for generating validity information for a

                ~~packet~~packets comprising binding update messages, wherein the validity

                information for a packet comprises all necessary information required for

                performing a validity check of the packet and no pre-established security

                association is needed to verify the packet, and the validity information

                comprises algorithm information to be used to perform the validity check of

                the packet, wherein the algorithm information comprises values to initialize an

                algorithm to be used to perform the validity check of the packet, the validity

                information further comprising public key information of a sending node

                comprising address in a database of a server from which the public key of the

                sending node can be obtained;

        packet header generating means for generating ~~a header~~headers for the packets, the

                packet header generating means generating headers comprising the validity

                information for packets comprising binding update messages and generating

                headers without the validity information for packets not comprising the

                binding update messages; and

        sending means for sending the ~~packet~~packets including the corresponding

                headers~~header~~ to a receiving network node~~,~~

~~wherein the validity information comprises all necessary information required for performing a validity check of the packet and no pre-established security association is needed to verify the packet, and the validity information comprises algorithm information to be used to perform the validity check of the packet, wherein the algorithm information comprises values to initialize an algorithm to be used to perform the validity check of the packet, the validity information further comprising public key information of a sending node comprising address in a database of a server from which the public key of the sending node can be obtained.~~

19.-41. (Cancelled)

42.   (Currently Amended) An apparatus, comprising:

~~a validity information generator~~at least one processor configured to:

generate validity information for ~~a packet~~packets comprising binding update messages, wherein the validity information for a packet comprises all necessary information required to perform a validity check of the packet and no pre-established security association is needed to verify the packet, and the validity information comprises algorithm information to be used to perform the validity check of the packet, wherein the algorithm information comprises values to initialize an algorithm to be used to perform the validity check of the packet, the validity information further comprising public key information of a sending node comprising an address in a database of a server from which the public key of the sending node can be obtained;

a packet header generator configured to generate a headercorresponding headers for the packet, comprising the validity information for the packets comprising the binding update messages,;

generate corresponding packet headers without the validity information for packets not comprising the binding update messages; and

a transmitter configured to send the packet packets including the corresponding header headers to a receiving network node,

wherein the validity information comprises all necessary information required to perform a validity check of the packet and no pre-established security association is needed to verify the packet, and the validity information comprises algorithm information to be used to perform the validity check of the packet, wherein the algorithm information comprises values to initialize an algorithm to be used to perform the validity check of the packet, the validity information further comprising public key information of a sending node comprising an address in a database of a server from which the public key of the sending node can be obtained.

43.   (Previously Presented) The apparatus according to claim 42, wherein the validity information comprises security information indicating security services applied to the packet.

44.-49. (Cancelled)

50.   (Previously Presented) The apparatus according to claim 42, wherein the public key information comprises public key verification information indicating information in order to verify that the public key actually belongs to the sending node.

51.   (Previously Presented) The apparatus according to claim 42, wherein the validity information comprises an information item to prevent replay attacks.

52.   (Previously Presented) The apparatus according to claim 51, wherein the information item to prevent replay attacks contains an indication of a procedure to be used for anti-replay attacks.

53.   (Previously Presented) The apparatus according to claim 51, wherein the information item to prevent replay attacks contains a time stamp.

54.   (Currently Amended) The apparatus according to claim 42, ~~further comprising~~wherein the at least one processor is further configured to:

        ~~a signor configured to~~ sign the packet using a private key corresponding to a public
                key indicated by the validity information in the packet header in the sending
                network node.

55.   (Currently Amended) An apparatus, comprising:
        a receiver configured to receive packets from a sending network node; and

        ~~a checker~~at least one processor configured to:

        perform ~~a~~ validity checks of ~~a packet~~ received packets comprising binding update
                messages and corresponding validity information contained in headers of the

7

received packets by referring to the validity information ~~contained in a header~~
~~of the packet~~,

wherein the validity information comprises all necessary information required to

perform ~~the~~ a validity check of ~~the~~ a received packet and no pre-established

security association is needed to verify the received packet, and the validity

information comprises algorithm information to be used to perform the

validity check of the received packet, wherein the algorithm information

comprises values to initialize an algorithm to be used to perform the validity

check of the received packet, the validity information further comprising

public key information of a sending node comprising an address in a database

of a server from which the public key of the sending node can be obtained,

processing the received packets comprising the binding update messages at least
according to the validity checks, and

processing received packets not comprising the binding update messages without
validity checks.

56.   (Previously Presented) The apparatus according to claim 55, wherein the validity
information comprises security information indicating security services applied to the packet.

57.-58. (Cancelled)

59.   (Currently Amended) An apparatus, comprising:
        a receiver configured to receive packets from a sending network node,

        a transmitter configured to forward packets received from ~~a~~ the sending network node
                to a receiving network node; ~~and~~,

a checker at least one processor configured to to:

perform a validity checks of a packetreceived packets comprising binding update
messages and corresponding validity information contained in headers of the
received packets by referring to the validity information contained in a header
of the packet,

wherein the validity information comprises all necessary information required to
perform a validity check of the a received packet and no pre-established
security association is needed to verify the received packet, and the validity
information comprises algorithm information to be used to perform the
validity check of the received packet, wherein the algorithm information
comprises values to initialize an algorithm to be used to perform the validity
check of the received packet, the validity information further comprising
public key information of a sending node comprising an address in a database
of a server from which the public key of the sending node can be obtained,

causing received packets comprising the binding update messages and meeting the
validity checks to be forwarded to the receiving network node, and

causing received packets not comprising the binding update messages and
corresponding validity information to be forwarded to the receiving network
node without validity checks.

60. (Previously Presented) The apparatus according to claim 59, wherein the validity
information comprises security information indicating security services applied to the packet.

61.-62. (Cancelled)

63.   (Currently Amended) A method, comprising:

receiving packets at a network node; and

performing a validity checks of a packetreceived packets comprising binding update
messages and corresponding validity information contained in headers of the
received packets by referring to the validity information contained in a header
of the packet,

wherein the validity information comprises all necessary information required for
performing the a validity check of the a received packet and no pre-established
security association is needed to verify the received packet, the validity
information comprising algorithm information to be used for performing the
validity check of the received packet, wherein the algorithm information
comprises values to initialize an algorithm to be used to perform the validity
check of the received packet, the validity information further comprising
public key information of a sending node comprising an address in a database
of a server from which the public key of the sending node can be obtained,

processing the received packets comprising the binding update messages at least
according to the validity checks, and

processing received packets not comprising the binding update messages without
· validity checks.

64.   (Currently Amended) A method, comprising:
receiving packets from a sending network node,

forwarding received packets to a receiving network node; and,

performing a validity checks of received packets comprising binding update messages
and corresponding validity information contained in headers of the received

packets~~a packet~~ by referring to the validity information ~~contained in a header of the packet~~,

wherein the validity information comprises all necessary information required for performing a validity check of ~~the~~ a received packet and no pre-established security association is needed to verify the received packet, the validity information comprising algorithm information to be used for performing the validity check of the received packet, wherein the algorithm information comprises values to initialize an algorithm to be used to perform the validity check of the received packet, the validity information further comprising public key information of a sending node comprising an address in a database of a server from which the public key of the sending node can be obtained,

causing received packets comprising the binding update messages and meeting the validity checks to be forwarded to the receiving network node, and

causing received packets not comprising the binding update messages and corresponding validity information to be forwarded to the receiving network node without validity checks.

65.   (Cancelled)

66.   (Currently Amended) A non-transitory computer readable storage medium with an executable computer program stored thereon, wherein the computer program instructs a processor to perform:

for packets comprising binding update messages:

generating validity information for ~~a~~ the packets, wherein the validity information for a packet comprises all necessary information required

to perform a validity check of the packet and no pre-established security association is needed to verify the packet, the validity information comprising algorithm information to be used to perform the validity check of the packet, wherein the algorithm information comprises values to initialize an algorithm to be used to perform the validity check of the packet, the validity information further comprising public key information of a sending node comprising an address in a database of a server from which the public key of the sending node can be obtained; and

generating a packet header, comprising the validity information; ~~and~~

for packets not comprising the binding update messages, generating a packet header without the validity information; and

sending ~~the~~ packets including the corresponding packet headers ~~from a first network node~~ to a ~~second~~ receiving network node.

67.   (Currently Amended) A non-transitory computer readable storage medium with an executable computer program stored thereon, wherein the computer program instructs a processor to perform:

receiving packets at a network node; and

performing ~~a~~ validity checks of received packets comprising binding update messages and corresponding validity information contained in headers of the received packets~~a packet~~ by referring to the validity information ~~contained in a header of the packet,~~

wherein the validity information comprises all necessary information required for performing ~~the~~a validity check of ~~the~~a received packet and no pre-established

security association is needed to verify the received packet, the validity
information comprising algorithm information to be used for performing the
validity check of the received packet, wherein the algorithm information
comprises values to initialize an algorithm to be used to perform the validity
check of the received packet, the validity information further comprising
public key information of a sending node comprising an address in a database
of a server from which the public key of the sending node can be obtained,

processing the received packets comprising the binding update messages at least
according to the validity checks, and

processing received packets not comprising the binding update messages without
validity checks.

68.   (Currently Amended) A non-transitory computer readable storage medium with an
executable computer program stored thereon, wherein the computer program instructs a
processor to perform:

receiving packets from a sending network node,

forwarding received packets to a receiving network node; and,

performing a-validity checks of received packets comprising binding update messages
and corresponding validity information contained in headers of the received
packetsa packet by referring to the validity information contained in a header
of the packet,

wherein the validity information comprises all necessary information required for
performing a validity check of the a received packet and no pre-established
security association is needed to verify the received packet, the validity
information comprising algorithm information to be used for performing the

validity check of the <u>received</u> packet, wherein the algorithm information comprises values to initialize an algorithm to be used to perform the validity check of the <u>received</u> packet, the validity information further comprising public key information of a sending node comprising an address in a database of a server from which the public key of the sending node can be obtained,

<u>causing received packets comprising the binding update messages and meeting the validity checks to be forwarded to the receiving network node, and</u>

<u>causing received packets not comprising the binding update messages and corresponding validity information to be forwarded to the receiving network node without validity checks.</u>

69.   (New) The method according to claim 1, wherein generating further comprises generating validity information further comprising a pointer comprising an address of a database within a server to access a certificate used to verify validity of the packet.